HandsOn Connect and the EU General Data Protection Regulation (GDPR)

This article is intended for HandsOn Connect (HOC) customers that are affected by the General Data Protection Regulation (GDPR) going into effect on May 25th, 2018. It is not legal advice, just some information we believe might help.

HandsOn Connect (HOC) is committed to your privacy, keeping your personal data secure, and compliance with the General Data Protection Regulation (GDPR) which goes into effect on May 25th, 2018. GDPR is a major step in protecting the privacy of European Union (EU) residents, giving them more control over what, how, why, where, and when their personal data is used.

HOC has also updated its privacy policy and it can be reviewed here:

https://www.handsonconnect.org/privacy-policy

For illustrative purposes only, we have also provided a sample of a GDPR Notice you can use to get started with your own notice:

Simple GDPR Notice (Sample)

Let's start by briefly describing what is what, who is who and who does what, because GDPR is extensive and depending on the role you play in interacting with the user data, you have different obligations.

First, let's understand some key terms related to the GDPR, as defined by the UK's Information Commissioner's website:

Term	Definition
Personal data	Means data which relate to a living individual who can be identified: • from those data, or • from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual
Sensitive personal data	Sensitive personal data means personal data consisting of information as to: • the racial or ethnic origin of the data subject, • his political opinions, • his religious beliefs or other beliefs of a similar nature,

Term	Definition
	• whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), • his physical or mental health or condition, • his sexual life, • the commission or alleged commission by him of any offense, or • any proceedings for any offense committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.
Data Subject	Means an individual who is the subject of personal data. In the context of HOC is usually means a user that has a registered account created through or used in HOC (e.g., volunteer, partner).
Data Controller	A person who (either alone or jointly or in common with other persons) or entity that determines the purposes for which and the manner in which any personal data are, or are to be, processed. **If you are an individual or entity that uses HOC to deliver services to users, you are a Data controller.**
Data Processor	In relation to personal data means any person (other than an employee of the data controller) or entity who processes the data on behalf of the Data Controller. HOC is a Data Processor to those individuals and entities who use our services for the process of delivering services to users who are registered on a HandsOn Connect instance.
Third-party	In relation to personal data means any person or entity other than: • the Data Subject, • the Data Controller, or • any Data Processor or other person authorized to process data for the data controller or processor.

Based on the definitions above, since HOC is a Software-as-a-Service (SaaS) and we process our client's data, in GDPR lingo we are known as a Data Processor. **Our clients control the use of their user's data. Hence a HOC client will more likely be a Data Controller.**

1. What do you need to know as a HOC client and Data

Controller?

As a HOC client, and a Data Controller, who uses HOC to provide users (e.g., volunteers, partners) with services, and captures their information, especially if the user is an EU resident, there certain things you are responsible for under GDPR. We attempt to simplify them here, but please make sure to review the GDPR act and consult with your legal counsel.

First, understand that **as HOC client you are most likely a Data Controller**, since you, alone or with others, "determine the purposes for which and the manner in which any personal data are processed". As such you remain responsible for ensuring the processing complies with the Act, whether you do it in-house or engage a Data Processor (e.g., HOC, Salesforce, Click & Pledge, MailChimp).

Ad HOC customer, it is likely that your main system is Salesforce, hence a lot of what you need to do to comply with GDPR is tied to Salesforce. To learn more go to:

https://www.salesforce.com/eu/campaign/gdpr/

To help meet the Data Controller requirements for GDPR, there are a couple of things you can do:

Obligation	What you can do...
Obtaining Data Subject Consent A Data Subject (e.g., volunteer, partner) must be presented with the option to provide consent for the collection, processing, and storage of their personal information in an intelligible format in an easily accessible form. Consent must provide clear and distinguishable information, in plain language, that accurately describes the purpose for which consent is being granted. Additionally, consent must be withdrawable in an easily accessible form.	• Use in HOC the Privacy Policy and Terms and Conditions pages. • Use in HOC the Advanced Registration and Sign-up Module to present additional information, consent, workflow and opt-in options.
Ability to Withdraw Data Subject Consent A Data Subject (e.g., volunteer, partner) must be presented with the option to withdraw consent in an easily accessible form.	• Use the HOC Form Builder to create an easily accessible form to withdraw consent. • Use clear and concise language, such as "By using our Site, App or service, you consent to our Privacy Policy. If you don't agree, please don't use our Site, App or Service."

Right to Be Forgotten

This is probably the best-known obligation. Data Subjects have the right to have their personal data removed from the systems of controllers and processors under some circumstances, such as by removing their consent for its processing.

Salesforce provides all the necessary tools to make sure you can erase the data for a user. This task can take several steps and may vary, depending on the complexity of your contact record, if you keep user data in other objects, the different apps that use the data, and any integrations you might have internally or with third-parties.

Salesforce allows customers to delete personal data at both an organizational level and an individual level. For more information, please see:

https://help.salesforce.com/articleView?id=data_deletion_platform.htm&type=5

Accountability/Transparency

The processor shall take appropriate measures to provide any information referred to in Chapter 3 and any communication under this article related to the data subject.

HOC as a data processor will provide any information related to:

- personal data accuracy
- data subject data collection,
- data subject accessibility,
- data rectification or erasure,
- notification,
- data portability, and
- restrictions

Data Portability

Data subjects also now have the right, in certain circumstances, to receive the personal data that they have provided to a controller in a structured, commonly used and machine-readable format.

HOC as a processor will provide the personal data concerning of their data subjects through controllers. The data subject and/or controller will be able to re-transmit those data to another controller. However, the last action should be under data subjects and controller responsibility based on HandsOn Connect Terms of Use letter E.

Right to the restriction of processing

Restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling, as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers may be imposed by Union or Member State law.

Provide a mechanism; even if it is a way to submit a written request, to allow your users to opt-out:

- processing based on legitimate interests or the performance of a task in the public interest/ exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

2. What is HOC doing regarding GDPR and its role as a Data Processor?

At HOC we have always taken data privacy and protection very seriously, by meeting the industry standards by building our application on platforms, such as Salesforce and Azure, certified with industry standards, such as ISO 27001, SOC 2 Type 2, and EU-U.S. Privacy Shield, as well as compliant with GDPR.

Since HOC is a Salesforce App and HOC uses Salesforce as the primary data storage, we are fortunate that this effort is greatly facilitated because many of the Data Processor requirements are provided by and through Salesforce. To learn more about Salesforce's GDPR compliance, please visit:

https://www.salesforce.com/gdpr/platform/

We are committed to addressing EU data protection requirements applicable to us as a Data Processor. To this effect we are:

- **Identifying personal data**: we have audited the default collection of personal data, as well as its usage, storage, and disposal.
- **Providing visibility and transparency**: As a Data Processor, HOC's key role is to provide our clients (i.e., Data Controllers) with the tools and access to effectively manage and protect their user data, as described in section 1 of this document.
- **Enhancing data integrity and security**: As our customers tighten their data security measures, we are doing the same, by implementing IT policies and procedures that provide end-to-end security.
- **Portability and transferability of data**: Leveraged by using Salesforce to comply with the user's the right to either receive all the data provided and processed by the controller or transfer it to another controller depending on technical feasibility, as described in section 1 of this document.

Data Sub-processors used by HandsOn Connect

HOC uses several systems, technologies, and tools to deliver its services. We maintain the following list of sub-processors:

- Salesforce: Customer Relationship Management. United States.
- Microsoft Azure: Application hosting. United States.
- QuickBooks: Customer invoicing, payment processing and credit card processing. United States.
- Google Analytics: Application analytics. United States.
- Jira: Development issue tracking and reports. United States.
- Raygun: Error, Crash & Performance Monitoring For Web & Mobile Apps. United States.
- Logentries: Application Logs. United States.
- Zendesk: Customer support and documentation. United States.
- Hootsuite: Social media management. United States.
- All for Good (Points of Light): Volunteer opportunity aggregator and search. United States.

- Cabot Volunteer Rewards: Opt-in rewards program for volunteers. United States.
- Squarespace. Website host. United States.

Wrap up

If GDPR affects you, it will take some time and work to comply, if you haven't already. In the end, we believe that the GDPR is a positive for both individuals and organizations.

Although we cannot implement GDPR for you, If you have any questions contact us at dataprotection@handsonconnect.org. Remember to consult with your legal counsel.